FACSIMILE COVER SHEET

The Law Offices of
STRAUB & POKOTYLO

620 Tinton Avenue
Bldg. B, 2nd Floor
Tinton Falls, NJ 07724-3260

Telephone: 732-542-9070
Facsimile: 732-542-9071
Internet site: www.sp-ip.com

To: **U.S. Patent and Trademark Office**

Facsimile No.: **(571) 273-8300**

Telephone No.: _____

From: **Michael P. Straub, Esq.**

Date: **March 17, 2008**

Number of Pages Including Cover: 30

MESSAGE: **FORMAL SUBMISSION OF:**
1) Fee Transmittal (in duplicate); and
2) Appeal Brief

Attorney Docket No.: **Verizon-36 (03-1506)**
Appl. No.: **10/678,328**
Applicant: **Gaston S. Ormazabal**
Filed: **October 3, 2003**
Title: **NETWORK FIREWALL TEST METHODS AND APPARATUS**
TC/A.U.: **2136**
Examiner: **Brandon S. Hoffman**

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this paper (and any accompanying paper(s)) is being facsimile transmitted to the United States Patents and Trademark Office on the date shown below.

Michael P. Straub
Type or print name of person signing certification

Michael P Straub
Signature

March 17, 2008
Date

Modified PTO/SB/17 (01-03)
Approved for use through 04/30/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2007

Effective 09/30/2007. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 510.00

Complete if Known	
Application Number	10/678,328
Filing Date	October 3, 2003
First Named Inventor	Gaston S. Ormazabal
Examiner Name	Brandon S. Hoffman
Art Unit	2136
Attorney Docket No.	Verizon-36 (03-1506)

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 50-1049

Deposit Account Name: Straub & Pokotylo

The Commissioner is authorized to: *(check all that apply)*

☒ Charge any fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) due in connection with the filing submitted herewith

☐ Charge fee(s) indicated below, **except for the filing fee** in the to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING, SEARCH & EXAMINATION FEES

Large Entity Fee ($)	Small Entity Fee ($)	Fee Description	Fee Paid
1030	515	Utility fee	
440	220	Design fee	
680	340	Plant fee	
1440	720	Reissue fee	
210	105	Provisional fee	

SUBTOTAL (1) ($) 0.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =	X	=
Independent Claims		- 3** =	X	=
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	210	2201	105	Independent claims in excess of 3
1203	370	2203	185	Multiple dependent claim, if not paid
1204	210	2204	105	**Reissue independent claims over original patent
1205	50	2205	25	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

***or number previously paid, if greater, For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for ex parte reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	460	2252	230	Extension for reply within second month	
1253	1,050	2253	525	Extension for reply within third month	
1254	1,640	2254	820	Extension for reply within fourth month	
1255	2,230	2255	1,115	Extension for reply within fifth month	
1401	510	2401	255	Notice of Appeal	
1402	510	2402	255	Filing a brief in support of an appeal	510.00
1403	1,030	2403	515	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	510	2452	255	Petition to revive - unavoidable	
1453	1,540	2453	770	Petition to revive - unintentional	
1501	1,440	2501	720	Utility issue fee (or reissue)	
1502	820	2502	410	Design issue fee	
1503	1,130	2503	565	Plant issue fee	
				Petitions to the Commissioner – check fee sheet	
1807	50	1807	50	Processing fee under 37 CFR 1.17(c)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	810	2809	405	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	810	2810	405	For each additional invention to be examined (37 CFR 1.129(b))	
1801	810	2801	405	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 510.00

SUBMITTED BY				(Complete *if applicable*)	
Name (Print/Type)	Michael P. Straub	*Registration No. (Attorney/Agent)*	36,941	*Telephone*	(732) 542-9070
Signature	Michael P. Straub			*Date*	March 17, 2008

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Attorney Docket No.: **Verizon-36 (03-1506)**

Appl. No.: **10/678,328**

Appellants: **Gaston S. Ormazabal**

Filed: **October 3, 2003**

Title: **NETWORK FIREWALL TEST METHODS AND APPARATUS**

TC/A.U.: **2136**

Examiner: **Brandon S. Hoffman**

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Further to the Notice of Appeal filed on January 24, 2008, which set a deadline for submission of this Appeal brief to expire on March 24, 2008, the appellant requests that the Board reverse all outstanding grounds of rejection in view of the following.

I. Real Party In Interest

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

II. Related Appeals and Interference

There are no related appeals or interferences.

III. Status of Claims

Claims 1-14 are pending.

Claims 1-14 are rejected. Specifically, claims 1-7 and 9-13 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003/0195861 to McClure et al. (hereinafter "the McClure et al. publication") in view of U.S. Patent Publication No. 2003/0115321 to Edmison et al. (hereinafter "the Edmison et al. publication"). In addition claims 8 and 14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the McClure et al. publication in view of the Edmison et al. publication , and further in view of U.S. Patent Publication No. 2004/0028035 to Read (hereinafter "the Read publication").

The foregoing rejections of claims 1-14 are appealed.

IV. Status of Amendments

No amendments have been made, and no new matter has been introduced.

V. Summary of the Claimed Subject Matter

One aspect of the present invention concerns the testing of a firewall. In particular, the method recited in claim 1 includes transmitting a communications session initiation signal from a signal source using an IP address corresponding to the signal source to establish a communications session to be conducted through the firewall, transmitting test signals following initiation of the communications session and prior to termination of the initiated communications session, at a range of ports in a first side of the firewall through which media signals may be transmitted when the ports are open, the test signals including the IP address, monitoring a second side of the firewall to detect any transmitted test signals that pass through the firewall, and identifying any open ports that are not associated with the established communications session, which passed at least one of the transmitted test signals, as erroneously open ports (This is supported, for example, by Figure 5A, 510 and page 35, lines 20-27; Figure 5A, 512 and page 36, lines 7-10; Figure 5A, 514 and page 36, lines 10-14; and Figure 5A, 516 and page 36, lines 17-22). In some

embodiments, the transmitted test signals are IP packets which include the IP address as a source address (This is supported, for example, by Figure 5A, 512 and page 36, lines 7-10).

In some embodiments, the method further comprises determining from at least one session initiation signal at least one port associated with the established communication session that should be open, and generating an error signal indicating that at least one port associated with the established communication session is erroneously closed if a test signal is not detected passing through the port to the second side of the firewall (This is supported, for example, by Figure 5A, 516 and page 36, lines 17-22).

In still other embodiments, one method recites, prior to transmitting the communications session initiation signal, transmitting a first test signal at the first side of the network firewall from the signal source using an IP address that is not associated with any ongoing communications session being conducted through the firewall; monitoring the second side of said firewall to determine if the first test signal passed through the firewall; and reporting a firewall error if it is determined that the first signal passed through the firewall (This is supported, for example, by Figure 5A, 504 and page 35, lines 2-6; Figure 5A, 506 and page 35, lines 9-11; and Figure 35, 518 and page 35, lines 12-15).

Still other embodiments include having the transmitting steps performed by a first test device and the monitoring steps performed by a second test device, the second test device being physically separate from the first test device, and wherein the method further

comprises synchronizing the first and second test devices to a common clock located external to the first and second test devices (This is supported, for example, by Figure 1, 260 and page 25, line 1 thru page 26, line 4).

Still other embodiments include operating the first test device to communicate information identifying ports through which test signals were detected passing through the firewall from the second side to the second test device, and operating the second test device to generate a test report including information about the status of unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the first side. Further, some embodiments further comprise operating the second test device to communicate information identifying ports through which test signals were detected passing through the firewall from the first side to the first test device, and operating the first test device to generate a test report including information about the status of unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the first side (This is supported, for example, by Figure 3, 168 and page 26, lines 4-11).

To summarize the foregoing, various embodiments of the present invention may be used to utilize test devices to send and receive signals through a firewall in order to determine whether ports in the firewall are operating correctly.

VI. Grounds of Rejection to be Reviewed on Appeal

The issues presented for review are whether:

(1) (separately patentable and argued groups of) claims 1-7 and 9-13 are rendered obvious by the McClure et al. publication" in view of the Edmison et al. publication; and

(2) (separately patentable and argued groups of) claims 8 and 14 are rendered obvious by the McClure et al. publication in view of the Edmison et al. publication , and further in view of the Read publication.

VII. Argument

The appellant respectfully requests that the Board reverse the final rejection of claims 1-14 in view of the following.

Rejections under 35 U.S.C. § 103

Group I: Claims 1, 2, 9, 10, and 14

Claims 1, 2, 9, and 10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the McClure et al. publication in view of the Edmison et al. publication. Claim 14 stands rejected under 35 U.S.C. §103(a) as being unpatentable over the McClure et al. publication in view of the Edmison et al. publication ,

and further in view of the Read publication. The appellant respectfully requests that the Board reverse these grounds of rejection in view of the following.

Independent Claim 1 is representative of Claim Group I and contains the following features (emphasis added):

> *A method of testing a network firewall, comprising:*
> ***transmitting a communications session initiation signal from said signal source using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall;***
> ***transmitting test signals from said signal source, following initiation of said communications session and prior to termination of said initiated communications session, at a range of ports in a first side of said firewall through which media signals may be transmitted when said ports are open, said test signals including said IP address;***
> ***monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall;*** *and*
> ***identifying any open ports that are not associated with said established communications session,*** *which passed at least one of said transmitted test signals,* ***as erroneously open ports.***

The Examiner acknowledges on p. 3 of the Final Office Action, dated October 24, 2007, that:

> "McClure et al. does not teach ….a second test device located on a trusted side of said firewall, the second test device including: means for monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall and an analysis module for identifying any open ports that are not associated with an established communications session, which passed at least

> one of said transmitted test signals, as erroneously open ports."

The Examiner goes on to state that (emphasis added):

> "Edmison et al. teaches … a second test device located on a trusted side of **said firewall**, the second test device including (fig. 1, ref. num 10 and 20): means for monitoring a second side of **said firewall** to detect any transmitted test signals that pass through **said firewall** (paragraph 0040) and **an analysis module for identifying any open ports that are not associated with an established communications session, which passed at least one of said transmitted test signals, as erroneously open ports** (paragraph 0010)."

First, there is no mention of a **firewall** in the cited references of the Edmison et al. publication. Fig. 1 shows a "first network element" 10; and a "second network element 20", a "user card 31", and a "user destination 29" at the distant end of the network being tested. Fig. 2 shows a "network element" 10, with "ingress user port(s)" 52 and 54, and "egress user port(s)" 49 and 56. There is no mention of "firewalls". Neither paragraph 10 nor paragraph 40 mentions a "firewall".

The Edmison et al. publication discloses (abstract):

> "a method which involves inserting probe packets on a per service basis for transmission on a respective round trip; and for each service using the probe packets to calculate packet latency for probe packets which is representative of packet latency for all packets transmitted for the service. In some embodiments, data plane time stamps are used to accurately time probe latency. The invention also provides a method which involves inserting probe packets on a per service basis for

> transmission on a respective destination network element; and at the destination network element for a given service using the probe packets to calculate one way packet loss for the service".

As can be seen, the Edmison et al. publication teaches sending probe packets to a destination and back to the origination, while monitoring to see how long this process takes, and whether any packets are dropped. There is no suggestion of testing a **firewall**.

The Examiner states on page 8: "the word firewall does not need to appear so long as there is an item that acts and behaves like a firewall present in the network". The Examiner also states: "McClure is the reference cited for actually teaching testing a firewall, as shown in figure 1." Applicant continues to maintain that the Edmison et al. publication tests network latency by sending and receiving probes from various places in a network, without targeting (or even mentioning) firewalls. Therefore, it does not follow that the McClure et al. publication teachings would be incorporated into the Edmison et al. publication teachings for "*monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall*".

Second, there is no teaching or suggestion in the Edmison et al. publication of "***identifying any open ports that are not associated with said established communications session***". The Edmison et al. publication discloses, at paragraph 0040:

> "Each packet received at an ingress user port belonging to a given service is typically given a certain treatment, and forwarded to an appropriate egress network port. A count of these packets is maintained for each service."

It can be seen that ports are selected for use as ingress and egress ports for probe packets, and there is no teaching or suggestion of looking for or identifying open ports **of a firewall that are not associated** with the testing probe transmissions and receptions ("established communications session").

Further, there is no teaching or suggestion in the Edmison et al. publication of identifying any ports "***as erroneously open ports***". There is no mention of "erroneously open ports" in the Edmison et al. publication, to say nothing of "identifying" them.

Neither the McClure et al. publication nor the Edmison et al. publication teach or suggest the features of claim 1 of:

> *identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports*

Therefore, no combination of the McClure et al. publication and the Edmison et al. publication teach or suggest the above feature of claim 1.

The Examiner states on page 8: "McClure teaches, at paragraph 0130, that TCP packets are sent to all ports and packets that get a timeout are in response to closed ports." The Examiner then states, regarding the Edmison et al. publication: "The packets are considered erroneous when they non-conform". However, neither statement refers to "erroneously open ports". The McClure et al. publication teaches identifying open ports, and the Edmison et al. publication identifies non-conforming **packets**. Therefore, no combination of the references

teaches or suggests "*identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports*".

Further, the McClure et al. publication teaches testing ports by sending signals toward the ports, and identifying **responses to those signals from the target device**. At paragraph 11 it states: "The system and method can be run remotely from a monitoring computer outside the target network, or can be run by a monitoring computer included within the target network".

The Edmison et al. publication teaches transmitting and receiving probes at various places in the network, in order to determine network latency (with associated timing functionality). However, practitioners of the McClure et al. publication, knowing of the Edmison et al. publication, would not choose to incorporate the topology of the Edmison et al. publication into their topology. If someone **suggested** to them that they place devices on the second side of each firewall in each target computer, the response would be that there would be no reason to do so, and that such a solution would be **less** economical than the solution taught by the McClure et al. publication.

Further, even if one **wanted** to incorporate the Edmison et al. publication teachings into the McClure et al. publication system, there is no teaching of how the the McClure et al. publication system should be modified to accomplish such an integration of systems.

Third, neither the McClure et al. publication nor the Edmison et al. publication teach or suggest "*transmitting test signals from said signal source,*

following initiation of said communications session and prior to termination of said initiated communications session". Both the McClure et al. publication and the Edmison et al. publication teach sending multiple signals simultaneously. Neither teaches or suggests "*transmitting a communications session initiation signal from said signal source using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall"*, followed by "*transmitting test signals from said signal source, following initiation of said communications session and prior to termination of said initiated communications session"*.

Further, neither reference teaches "*identifying any open ports that are not associated with said established communications session"*. Again, neither the McClure et al. publication nor the Edmison et al. publication teach or suggest identifying open ports that are *not associated with said established communications session*, since neither references teaches a **communications session** separate from the testing signals.

Additionally, neither reference teaches or suggests "*identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports"*. Neither the McClure et al. publication nor the Edmison et al. publication identify open ports in relation to a specific established communications session in order to identify such open ports as erroneously open ports.

Finally, a feature of claim 1 is (emphasis added): "*transmitting a communications session initiation signal*

from said signal source ***using an IP address corresponding to said signal source*** *"* and *"said test signals including* ***said IP address"***. Neither reference teaches or suggests *"transmitting a communications session initiation signal"*

"to establish a communications session to be conducted through said firewall", *"transmitting test signals"*, wherein *"said test signals [include] said IP address"*, and *"identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports"*. Neither the McClure et al. publication nor the Edmison et al. publication compares an established communications session with test signal results to identify erroneously open ports. No combination of the references would teach or suggest any of the above features.

For at least these reasons, claim 1 is patentable over the cited references, and the rejection should be overturned.

Claim 2, for at least the reason of being dependent on allowable claim 1, is therefore patentable over the cited references, and its rejections should be reversed.

Independent claim 9 is patentable over the cited references for the same reasons as those argued above in relation to claim 1, and its rejection should be overturned.

Claims 10 and 14, for at least the reason of being dependent on allowable claim 9, are therefore patentable over the cited references, and their rejections should be reversed.

Group II: Claims 3, 4, 5, 7, 8, 12 and 13

Claims 3, 4, 5, 7, 12, and 13 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the McClure et al. publication in view of the Edmison et al. publication. Claim 8 stands rejected under 35 U.S.C. §103(a) as being unpatentable over the McClure et al. publication in view of the Edmison et al. publication , and further in view of the Read publication. The appellant respectfully requests that the Board reverse these grounds of rejection in view of the following.

Dependent Claim 3 is representative of Claim Group II and contains the following features (emphasis added):

> *determining from at least one session initiation signal at least one port associated with the established communication session* ***that should be open****; and*
> *generating an error signal indicating that said at least one port associated with the established communication session* ***is erroneously closed*** *if a test signal is not detected passing through said port to the second side of said firewall*

First, claim 3 is patentable for the reasons argued above in relation to claim 1. Further, the above features are also not taught or suggested in the cited references.

The Examiner states on p. 5 of the Final Office Action:

> "Means for generating an error signal indicating that said at least one port associated with the established communication session is erroneously closed if a test signal is not detected passing through said port to the second side of said firewall (see fig. 3, ref. num 339 of McClure et al.)."

The text associated with ref. num 339 is found at paragraph [0064] and states:

> "Those IP addresses for which no response is received by any method are, in one embodiment, added to a dead list 339 of hosts."

This reference simply refers to ports that are "closed". It does not relate to whether any ports are "erroneously closed", which is a feature of claim 3.

For at least this additional reason, **claim 3 is patentable over the cited references, and the rejection should be overturned.**

Claims 4, 5, 7, and 8, for at least the reason of being dependent on allowable claims 1 and 3, are therefore patentable over the cited references, and their rejections should be reversed.

Claim 11 is patentable over the cited references for the same reasons as those argued above in relation to claim 3, and its rejection should be overturned.

Claims 12 and 13, for at least the reason of being dependent on allowable claim 11, are therefore patentable over the cited references, and their rejections should be reversed.

Group III: Claim 6

Claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over the McClure et al. publication in view of the Edmison et al. publication. The appellant respectfully requests that the Board reverse these grounds of rejection in view of the following.

First, claim 6 is patentable for the reasons argued above in relation to claims 1 and 3. Further, the above features are also not taught or suggested in the cited references.

Dependent Claim 6 contains the following features (emphasis added):

> *operating the first test device to communicate information identifying ports through which test signals were detected passing through said firewall* ***from the second side to the second test device****; and*
> *operating the second test device to generate a test report including information about the status of* ***unidirectional ports used to communicate signals from the first side to the second side*** *and* ***unidirectional ports used to communicate signals from the second side to the first side.***

The Examiner states on p. 6 of the Final Office Action:

> "Operating the [second/first] test device to generate a test report including information about the status of unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the

> first side (see fig. 2, ref. num 212 of McClure et al.)"

Ref. num 212 of Fig. 2 simply shows a row of ports on a "target computer on a target network" (paragraph [0057]). Later in that paragraph is:

> "On an IP network, a packet can be received at any one of 65,536 logical ports 212 at the target computer 200."

There is no reference to "a first test device" and "a second test device". Possibly the Examiner intends that if there is one test device, there can be two test devices. However, this would still not suggest "*from the second side to the second test device*", nor "*unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the first side*". There is no mention at all of "unidirectional ports", or using two test devices to test them.

For at least this additional reason, **claim 6 is patentable over the cited references, and the rejection should be overturned.**

VIII. Claims appendix

An appendix containing a copy of the claims on appeal is filed herewith.

IX. Evidence appendix

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor is there any other evidence entered by the Examiner and relied upon by the appellants in the appeal.

X. Related proceedings appendix

There are no decisions rendered by a court of the Board in any proceeding identified in section II above pursuant to 37 C.F.R. § 41.38 (c) (1) (ii).

Conclusion

In view of the foregoing, the appellants respectfully submit that the pending claims are in condition for allowance. Accordingly, the appellants request that the Board reverse each of the outstanding grounds of rejection.

Any arguments made in this Appeal Brief pertain ***only*** to the specific aspects of the invention ***claimed***. Any arguments are made ***without prejudice to, or disclaimer of***, the appellant's right to seek patent protection of any unclaimed (e.g., narrower, broader, different) subject matter, such as by way of a continuation or divisional patent application for example.

March 17, 2008

Respectfully submitted,

Michael P. Straub Attorney
Reg. No. 36,941
Tel.: (732) 542-9070

Claims Appendix

Including Complete Listing of Claims

Appl. No.: 10/678,328

Set forth below is a complete listing of claims

Claim 1 (original): A method of testing a network firewall, comprising:

transmitting a communications session initiation signal from said signal source using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall;

transmitting test signals from said signal source, following initiation of said communications session and prior to termination of said initiated communications session, at a range of ports in a first side of said firewall through which media signals may be transmitted when said ports are open, said test signals including said IP address;

monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall; and

identifying any open ports that are not associated

with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports.

Claim 2 (original): The method of claim 1, wherein said transmitted test signals are IP packets which include said IP address as a source address.

Claim 3 (original): The method of claim 1, further comprising:

determining from at least one session initiation signal at least one port associated with the established communication session that should be open; and

generating an error signal indicating that said at least one port associated with the established communication session is erroneously closed if a test signal is not detected passing through said port to the second side of said firewall.

Claim 4 (original): The method of claim 3, further comprising, prior to transmitting said communications session initiation signal,

transmitting a first test signal at the first side of said network firewall from the signal source using an

IP address that is not associated with any ongoing communications session being conducted through said firewall;

monitoring the second side of said firewall to determine if said first test signal passed through said firewall; and

reporting a firewall error if it is determined that said first signal passed through said firewall.

Claim 5 (original): The method of claim 3, wherein said transmitting steps are performed by a first test device and said monitoring steps are performed by a second test device, the second test device being physically separate from said first test device, the method further comprising:

synchronizing the first and second test devices to a common clock located external to said first and second test devices.

Claim 6 (original): The method of claim 5, further comprising;

operating the first test device to communicate information identifying ports through which test signals were detected passing through said firewall from the

second side to the second test device; and

operating the second test device to generate a test report including information about the status of unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the first side.

Claim 7 (original): The method of claim 5, further comprising;

operating the second test device to communicate information identifying ports through which test signals were detected passing through said firewall from the first side to the first test device; and

operating the first test device to generate a test report including information about the status of unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the first side.

Claim 8 (original): The method of claim 7, wherein said session signal is at least one of SIP and H.323 compliant signals.

Claim 9 (previously presented): A firewall test system, comprising:

a first test device located on an untrusted side of said firewall, the first test device including:

i) a session signal generator for transmitting a communications session initiation signal using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall;

ii) a probe signal generator for generating test signals at a range of ports in a first side of said firewall through which media signals may be transmitted when said ports are open, said test signals including said IP address; and

iii) timing synchronization circuitry for synchronizing said session signal generator and said probe signal generator to at least one of another test device and a clock signal source located external to said first test device; and

a second test device located on a trusted side of said firewall, the second test device including:

means for monitoring a second side of said

firewall to detect any transmitted test signals that pass through said firewall; and

an analysis module for identifying any open ports that are not associated with an established communications session, which passed at least one of said transmitted test signals, as erroneously open ports.

Claim 10 (original): The system of claim 9, wherein said probe signal generator generates IP packets which include said IP address as a source address.

Claim 11 (original): The system of claim 9, wherein said analysis module includes:

means for determining from at least one session initiation signal at least one port associated with the established communication session that should be open; and

means for generating an error signal indicating that said at least one port associated with the established communication session is erroneously closed if a test signal is not detected passing through said port to the second side of said firewall.

Claim 12 (original): The system of claim 11, wherein the test signal generator of said first test device includes:

means for transmitting a first test signal at the first side of said network firewall from the signal source using an IP address that is not associated with any ongoing communications session being conducted through said firewall prior to said communications session initiation signal being generated.

Claim 13 (original): The system of claim 11, wherein said first test device further includes:

an analysis module for monitoring the second side of said firewall to determine if said first test signal passed through said firewall; and

a report generation module for reporting a firewall error if it is determined that said first signal passed through said firewall.

Claim 14 (original): The system of claim 9, wherein said session signal generates at least one of SIP and H.323 compliant signals.

Evidence Appendix

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor is there any other evidence entered by the Examiner and relied upon by the appellants in the appeal.

Related proceedings Appendix

There are no decisions rendered by a court of the Board in any proceeding identified in section II above pursuant to 37 C.F.R. § 41.38 (c) (1) (ii).